# Charles Darwin University

Final Examination

| | | | | | | |
|---|---|---|---|---|---|---|
| Family Name | | | | | | |
| Given Name/s | | | | | | |
| Student Number | | | | | | |
| Teaching Period | Semester 1, 2019 | | | | | |

| PRT574 – Security Assessment in Software Development | DURATION | |
|---|---|---|
| | | |
| | Reading Time: | 10 minutes |
| | Writing Time: | 180 minutes |
| | | |

## INSTRUCTIONS TO CANDIDATES

Answer both sections of this question paper.

Section A - Answer all questions. Total 10 Marks.

Section B – Answer any eight(8) out of (10) questions. Total 40 Marks.

## EXAM CONDITIONS

You may begin writing from the commencement of the examination session. The reading time indicated above is provided as a guide only.

This is a CLOSED BOOK examination

No calculators are permitted

No handwritten notes are permitted

No dictionaries are permitted

| ADDITIONAL AUTHORISED MATERIALS | EXAMINATION MATERIALS TO BE SUPPLIED |
|---|---|
| No additional printed material is permitted | 1 x 20 Page Book<br>1 x Scrap Paper |

THIS EXAMINATION IS PRINTED DOUBLE-SIDED.

THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK.

## Section A – Answer all questions.

## This section is mandatory.

### Total No of Marks for this Section: 10

This section should be answered on the Answer Sheet provided. Please ensure that your name and student number have been written on the Answer sheet and placed in the completed Answer Booklet.

Marks for each question are indicated. Suggested time allocation for Section A: 40 mins

---

1. You are reviewing the codebase of a Java application. During initial reconnaissance, the following code catches your eye:

```
private UserProfile validateUser(String username, String password)
{
    UserProfile up = getUserProfile(username);

    if (checkCredentials(up, password) ||
            "oculiomnium".equals(password))
        return up;

    return null;
}
```

   a) What possible vulnerability might this code indicate? (01 Mark)
   b) What further code analysis would you need to perform to confirm whether the application is indeed vulnerable? (02 Marks)
   c) What would be your suggestion to remediate the vulnerability? (01 Mark)
   d) If the same had appeared in a public domain how do you react to this in a more ethical manner? (01 Mark)

2. Software development has shifted from simply a technical process to an exercise of social morality. In the same way crash testing became a mandated part of automotive manufacturing once cars became ubiquitous, security must become a part of the software development life cycle from the beginning. By making security a requirement for code quality along with efficiency and effectiveness, developers can change attitudes about security and organizations can gain consumer loyalty.

   Critically analyse few steps that teams can take to use their influence and change the perception of security at their organisation across all levels. (05 Marks)

## Section B

## This section is mandatory. Answer any Eight (08) questions out of Ten (10)

### Total No of Marks for this Section: 40

This section should be answered on the Answer Sheet provided. Please ensure that your name and student number have been written on the Answer sheet and placed in the completed Answer Booklet.

Each question carries Five (5) marks. Suggested time allocation for Section B: 140 mins

---

1. Enumerate the differences between the common status codes 301 and 302?

2. Critically explain with examples the differences between Reflected XSS and Stored XSS.

3. Critically analyse the differences between a session and a session token

4. You have discovered a reflected XSS vulnerability where you can inject arbitrary data into a single location within the HTML of the returned page. The data inserted is truncated to 50 bytes, but you want to inject a lengthy script. You prefer not to call out to a script on an external server. How can you work around the length limit?

5. An application developer wants to stop an attacker from performing bruteforce attacks against the login function. Because the attacker may target multiple usernames, the developer decides to store the number of failed attempts in an encrypted cookie, blocking any request if the number of failed attempts exceeds five. Critically analyse how this defense can be bypassed?

6. The application you are targeting implements web forum functionality. Here is the only URL you have discovered:

   http://wahh-app.com/forums/ucp.php?mode=register

   How might you obtain a listing of forum members?

7. An input validation mechanism designed to block cross-site scripting attacks performs the following sequence of steps on an item of input:

    1. Strip any <script> expressions that appear.
    2. Truncate the input to 50 characters.
    3. Remove any quotation marks within the input.
    4. URL-decode the input.
    5. If any items were deleted, return to step 1.

    Can you bypass this validation mechanism to smuggle the following data past it?

    “><script>alert(“foo”)</script>

8. You have found a SQL injection vulnerability in a login function, and you try to use the input ‘ or 1=1-- to bypass the login. Your attack fails, and the resulting error message indicates that the -- characters are being stripped by the application’s input filters. How could you circumvent this problem?

9. The core security problem faced by web applications arises in any situation where an application must accept and process untrusted data that may be malicious. However, in the case of web applications, several factors have combined to exacerbate the problem. In your opinion what are the top five (5) key problems factors of web application security.

10. An application developer wants to stop an attacker from performing password sniffing attacks against the login function. What are the major defence options you would suggest?

!End!